LAB – 2

SANTHOSH KRISHNA R

21BCE1651

DES ALGORITHM CLIENT-SERVER CODE

Client.c

```java
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import java.io.*;
import java.net.Socket;
import java.util.Scanner;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;

class Client {
    public static void main(String[] args) {
        try {
            Scanner scanner = new Scanner(System.in);
            System.out.print("Enter a message to send to the server: ");
            String message = scanner.nextLine();

            Socket socket = new Socket("localhost", 12345);

            KeyGenerator keyGenerator = KeyGenerator.getInstance("DES");
            SecretKey secretKey = keyGenerator.generateKey();

            Cipher cipher = Cipher.getInstance("DES");
            cipher.init(Cipher.ENCRYPT_MODE, secretKey);
```

```
            byte[] encryptedMessage = cipher.doFinal(message.getBytes());

            OutputStream outputStream = socket.getOutputStream();
            ObjectOutputStream objectOutputStream = new
ObjectOutputStream(outputStream);
            objectOutputStream.writeObject(encryptedMessage);

            objectOutputStream.close();
            outputStream.close();
            socket.close();
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}
```

server.c

```
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import java.io.*;
import java.net.ServerSocket;
import java.net.Socket;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;

class Server {
    public static void main(String[] args) {
        try {
            ServerSocket serverSocket = new ServerSocket(12345);

            Socket socket = serverSocket.accept();

            InputStream inputStream = socket.getInputStream();
            ObjectInputStream objectInputStream = new
ObjectInputStream(inputStream);
            byte[] encryptedMessage = (byte[]) objectInputStream.readObject();
```

```java
        KeyGenerator keyGenerator = KeyGenerator.getInstance("DES");
        SecretKey secretKey = keyGenerator.generateKey();

        Cipher cipher = Cipher.getInstance("DES");
        cipher.init(Cipher.DECRYPT_MODE, secretKey);

        byte[] decryptedMessage = cipher.doFinal(encryptedMessage);

        System.out.println("Decrypted Message: " + new
String(decryptedMessage));

        objectInputStream.close();
        inputStream.close();
        socket.close();
        serverSocket.close();
    } catch (Exception e) {
        e.printStackTrace();
    }
  }
}
```

Output:

```
PS C:\Users\SANTHOSH>  & 'C:\Program Files\Java\jdk-21\bin\java.exe' '--enable-preview' '-XX:+ShowCode
ta\Local\Temp\vscodesws_e6052\jdt_ws\jdt.ls-java-project\bin' 'Client'
Enter a message to send to the server: SANTHOSH
PS C:\Users\SANTHOSH> 
```

```
PS C:\Users\SANTHOSH>  & 'C:\Program Files\Java\jdk-21\bin\java.exe' '--enable-preview' '-
ta\Local\Temp\vscodesws_e6052\jdt_ws\jdt.ls-java-project\bin' 'DES'
MESSAGE RECEIVED (Encrypted) - ↕???♣?¶???\
Decrypted Message - SANTHOSH
PS C:\Users\SANTHOSH>
```